## AMENDMENTS TO THE SPECIFICATION

Please delete the section entitled "SUMMARY OF THE INVENTION" in its entirety and substitute the following section therefor:

### SUMMARY OF THE INVENTION

[0021] The present invention, among other applications, is directed to solving these and other problems and disadvantages of the prior art. The present invention provides a superior technique for performing cryptographic operations within a microprocessor. In one embodiment, an apparatus for performing cryptographic operations is provided. The apparatus includes fetch logic, algorithm logic, and execution logic. The fetch logic is disposed within a microprocessor and is configured to receive a cryptographic instruction instruction, wherein the cryptographic instruction is one of the instructions in an application program being executed by as part of an instruction flow executing on said microprocessorthe microprocessor. The cryptographic instruction prescribes one of the cryptographic operations and one of a plurality of cryptographic algorithms. The algorithm logic is disposed within said microprocessorthe microprocessor and operatively coupled to the cryptographic instruction. The algorithm logic directs the microprocessor to execute the one of the cryptographic operations according to the one of a plurality of cryptographic algorithms. The execution logic is disposed within said microprocessor and operatively coupled to the algorithm logic. The execution logic executes the one of the cryptographic operations. The execution logic includes, in addition to an integer unit for executing integer operations prescribed by the application program, a cryptography unit for executing a plurality of cryptographic rounds required to complete the one of the cryptographic operations.

[0022] One aspect of the present invention contemplates an apparatus for performing cryptographic operations. The apparatus has a cryptography unit within a microprocessor and algorithm logic. The cryptography unit executes one of the cryptographic operations responsive to receipt of a cryptographic instruction within an instruction flow that prescribes the one of the cryptographic operations, where the cryptographic instruction is one of the instructions in an application program that are fetched from memory by fetch

Application No. 10800938 (Docket: CNTR.2072)
37 CFR 1.111 Amendment dated 02/03/2008
Reply to Office Action of 11/13/2007

logic in the microprocessor, and wherein the microprocessor includes an integer unit for executing integer operations prescribed by the application program.. The cryptographic instruction has an algorithm field that prescribes one of a plurality of cryptographic algorithms to be employed when executing the one of the cryptographic operations. The algorithm logic is disposed within the microprocessor and operatively coupled to the cryptography unit. The algorithm logic directs the microprocessor to perform the one of the cryptographic operations according to the one of the plurality of cryptographic algorithms.

[0023] Another aspect of the present invention provides a method for performing cryptographic operations in a device. The method includes, within a microprocessor, fetching an integer instruction from memory that prescribes an integer operation, where the integer instruction is part of an application program being executed by the microprocessor; within thewithin a microprocessor, fetching a cryptographic instruction from memory that prescribes one of a plurality of cryptographic operations and one of a plurality of cryptographic algorithms. whereithe cryptographic instruction is also part of the application program being executed by the microprocessor; within an integer unit in the microprocessor, executing the integer operation; and within a cryptography unit in . and within the microprocessor, executing the one of the cryptographic operations according to the one of the cryptographic algorithms.